



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

09/982,072

10/18/2001

Glen H. Mullen

09469.006001; 97.0003

7280

7590

12/12/2005

Rosenthol & Osha L.L.P.
1221 McKinney Street
Suite 2800
Houston, TX 77010

EXAMINER

HOFFMAN, BRANDON S

ART UNIT

PAPER NUMBER

2136

DATE MAILED: 12/12/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/982,072	Applicant(s) MULLEN ET AL.	
	Examiner Brandon S. Hoffman	Art Unit 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on ____.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-35 is/are pending in the application.
- 4a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) ____ is/are allowed.
- 6) ☒ Claim(s) 1-35 is/are rejected.
- 7) ☐ Claim(s) ____ is/are objected to.
- 8) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 10-18-01 & 1-18-02 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. ____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|--|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date <u>10-18-01 & 8-5-02</u> . | 6) <input type="checkbox"/> Other: ____ |

DETAILED ACTION

Claim Rejections - 35 USC § 112

1. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.
2. Claim 12 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.
3. Claim 12 recites the limitation "the signed message" in line 2. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.
5. Claims 1-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chen et al. (U.S. Patent No. 6,061,796) in view of Shrader et al. (U.S. Patent No. 6,772,341).

Regarding claims 1, 2, 5, 14-16, and 20-23, Chen et al. teaches a network system providing integration, comprising:

- A client computer (fig. 1A, ref. num 4);

Art Unit: 2136

- A server (fig. 1A, ref. num 1);
- A server-side cryptographic function providing cryptographic services located on the server (fig. 6, ref. num 23);
- A remote access switch providing an interface between the client computer and the server (fig. 6, ref. num 8);
- A client-side cryptographic function providing cryptographic services located on the client computer (fig. 6, ref. num 20);
- A dial-up client providing dialing services to access the remote access switch (fig. 2-5, ref. num 25);
- A custom script dynamically linked library providing an interface between the dial-up client and the client-side cryptographic function (col. 2, lines 45-61, col. 3, lines 38-53, and fig. 2-5, ref. num 22);
- A security device holding authentication information (col. 9, lines 1-10); and
- A security device reader attached to the client computer for reading the security device (col. 9, lines 1-10).

Chen et al. does not specifically teach a PKI-Bridge, or a directory service accessed by the server-side cryptographic function. However, Chen et al. does teach of the SmartGATE VPN for the server, which is directly attached to the server, and therefore functions as the PKI-Bridge. The SmartGATE VPN is responsible for receiving information to enable secure communications between either a) a client and server, or b) a client and another client.

Art Unit: 2136

Shrader et al. teaches a directory service accessed by the server-side cryptographic function (col. 9, lines 39-53).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine a directory service accessible by the server-side cryptographic function, as taught by Shrader et al., with the network system of Chen et al. It would have been obvious for such modifications because the directory service provides keys to the server-side cryptographic function; this enables the server direct access to the keys.

Regarding claim 3, Chen et al. as modified by Shrader et al. teaches wherein a certificate is stored on the security device (see col. 7, lines 13-21 of Shrader et al.).

Regarding claims 4, 17, and 30, Chen et al. as modified by Shrader et al. teaches wherein the security device is a smart card (see col. 9, lines 1-10 of Chen et al.).

Regarding claims 6 and 33, Chen et al. as modified by Shrader et al. teaches wherein the directory service is lightweight directory access protocol compliant (see col. 9, lines 39-53 of Shrader et al.).

Regarding claim 7, Chen et al. as modified by Shrader et al. teaches wherein the client-side cryptographic function and the server-side cryptographic function employ the same cryptographic scheme (see col. 11, lines 16-23 of Chen et al.).

Regarding claims 8 and 11, Chen et al. as modified by Shrader et al. teaches wherein the server-side cryptographic function uses a random number generator to generate a challenge string (see fig. 6, ref. num 61 of Chen et al.).

Regarding claim 9, Chen et al. as modified by Shrader et al. teaches wherein the client-side cryptographic function uses a random number generator to generate a response string (see fig. 6, ref. num 61 of Chen et al.).

Regarding claim 10, Chen et al. as modified by Shrader et al. teaches wherein the client-side cryptographic function generates a signed response string (see col. 2, lines 21-37 of Chen et al., the reference incorporated by reference refers to col. 5, lines 45-56 for signing a message).

Regarding claim 12, Chen et al. as modified by Shrader et al. teaches wherein the server-side cryptographic function verifies the signed message (see col. 2, lines 21-37 of Chen et al., the reference incorporated by reference refers to col. 5, lines 19-44 for verifying a signed message).

Regarding claims 13 and 19, Chen et al. as modified by Shrader et al. teaches wherein the dial-up client automates the authentication process using a hidden terminal operating in terminal mode (see fig. 2, ref. num 25 of Chen et al.).

Regarding claim 18, Chen et al. as modified by Shrader et al. teaches wherein the custom script dynamically linked library comprises a SDLogin component and a SDSSetupDial component (see col. 3, lines 16-28 of Chen et al., dial-up internet access requires a user to login).

Regarding claims 24-29, 34, and 35, Chen et al. teaches a method/apparatus of integrating via a dial-up interface, comprising:

- Sending session initiation information from a dial-up client to a server (col. 9, lines 42-53);
- Checking session initiation information by the server (col. 9, lines 53-59);
- Generating a challenge string by a server-side cryptographic function (fig. 6, ref. num 61);
- Forwarding the challenge string to a custom script dynamically linked library (fig. 2, ref. num 22, the server [23] sends the challenge to the winsock first);
- Forwarding the challenge string to a client-side cryptographic function from the custom script dynamically linked library (fig. 6, ref. num 61, the winsock [22] then forwards the challenge to the SmartGATE VPN);

- Utilizing a private key from a security device (col. 2, lines 21-37, the reference incorporated by reference refers to col. 3, lines 44-59 for using a private key of a smart card);
- Generating a response string (fig. 6, ref. num 61);
- Signing the response string with the private key of a dial-in user (col. 2, lines 21-37, the reference incorporated by reference refers to col. 5, lines 45-56 for signing a message);
- Forwarding a signed response string to the custom script dynamically linked library (fig. 2, ref. num 20 going through 22);
- Dividing the signed response string into packets (col. 8, lines 43-61);
- Forwarding packets to the server (col. 8, lines 52-56);
- Reconstructing the signed response string from packets (col. 8, lines 57-67);
- Forwarding a reconstructed signed response string to the server-side cryptographic function (col. 8, lines 52-56);
- Obtaining a public key of the dial-in user (col. 2, lines 21-37, the reference incorporated by reference refers to col. 1, lines 39-49 and col. 5, lines 30-44 for verifying by using a public key);
- Verifying the reconstructed signed response string using the server-side cryptographic function (col. 2, lines 21-37, the reference incorporated by reference refers to col. 5, lines 19-44 for verifying a signed message);
- Reading the security device by a security device reader (col. 9, lines 1-10);
- Forwarding the challenge string to the dial-up client (fig. 6, ref. num 61);

- Forwarding the challenge string to the server (fig. 1, ref. num 61); and
- Forwarding packets from the custom script dynamically linked library (fig. 2, ref. num 22, packets are forwarded from the DLL to the SmartGATE VPN on the client).

Chen et al. does not specifically teach a PKI-Bridge, or encoding and decoding the signed response string. However, Chen et al. does teach of the SmartGATE VPN for the server, which is directly attached to the server, and therefore functions as the PKI-Bridge. The SmartGATE VPN is responsible for receiving information to enable secure communications between either a) a client and server, or b) a client and another client.

Shrader et al. teaches encoding and decoding the signed response string (col. 11, lines 49-67).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine encoding and decoding the signed response string, as taught by Shrader et al., with the method/apparatus of Chen et al. It would have been obvious for such modifications because encoding the signed response string prevents attackers from “seeing” what the response should look like. This prevents replay-attacks.

Art Unit: 2136

Regarding claim 31, Chen et al. as modified by Shrader et al. teaches wherein the session initiation information comprises version information and a distinguished name (see col. 8, lines 9-51 of Shrader et al.).

Regarding claim 32, Chen et al. as modified by Shrader et al. teaches wherein the public key is stored on a directory service (see col. 7, lines 13-21 of Shrader et al.).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon Hoffman whose telephone number is 571-272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Branda Hoff

BH

CEL
Primary Examiner
AV 2131
12/18/05